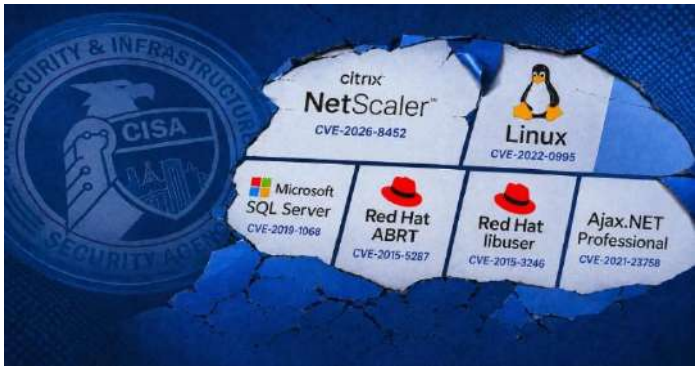
วันที่ 1 กันยายน 2569

CISA เพิ่มช่องโหว่ที่ถูกนำไปใช้โจมตีแล้ว 6 รายการในรายการ KEV รวมช่องโหว่ NetScaler, Linux และ SQL Server



สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) เมื่อวันพุธที่ผ่านมา ได้เพิ่มช่องโหว่ 6 รายการลงในรายการ Known Exploited Vulnerabilities (KEV) โดยหนึ่งในนั้นคือช่องโหว่ระดับความรุนแรงสูงที่ส่งผลกระทบต่อ Citrix NetScaler ADC และ NetScaler Gateway หลังพบหลักฐานว่าช่องโหว่ดังกล่าวกำลังถูกนำไปใช้โจมตีจริง ช่องโหว่มีรายละเอียดดังต่อไปนี้

- **CVE-2019-1068** - ช่องโหว่ Remote Code Execution ใน Microsoft SQL Server ซึ่งอาจเปิดทางให้ผู้โจมตีสามารถสั่งให้ระบบรันโค้ดภายใต้สิทธิ์ของบัญชีบริการ SQL Server Database Engine ได้
- **CVE-2026-8452** - ช่องโหว่ที่เกิดจากการจำกัดการทำงานภายในขอบเขตของ Memory Buffer ไม่ถูกต้องใน Citrix NetScaler ADC และ NetScaler Gateway ซึ่งอาจทำให้เกิดการโจมตีแบบ Denial-of-Service ได้
- **CVE-2022-0995** - ช่องโหว่ Out-of-Bounds Memory Write ใน Linux Kernel ซึ่งอาจเปิดทางให้ผู้ใช้ภายในเครื่องได้รับสิทธิ์ระดับสูง หรือทำให้ระบบเกิด Denial-of-Service ได้
- **CVE-2015-5287** - ช่องโหว่ยกระดับสิทธิ์ใน Red Hat Automatic Bug Reporting Tool (ABRT) ซึ่งอาจเปิดทางให้ผู้ใช้ภายในเครื่องที่มีสิทธิ์บางระดับสามารถเพิ่มสิทธิ์ของตนเองผ่านการโจมตีแบบ Symlink กับไฟล์ที่มีชื่อที่คาดเดาได้
- **CVE-2015-3246** - ช่องโหว่ Race Condition ใน Red Hat libuser ซึ่งอาจเปิดทางให้ผู้ใช้ภายในเครื่องที่ผ่านการยืนยันตัวตนแล้วสามารถทำให้ไฟล์ /etc/passwd เสียหาย ส่งผลให้เกิด Denial-of-Service หรือการยกระดับสิทธิ์ได้
- **CVE-2021-23758** - ช่องโหว่ Deserialization of Untrusted Data ใน Ajax.NET Professional (AjaxPro) ซึ่งอาจเปิดทางให้ผู้โจมตีสามารถรันโค้ดจากระยะไกลผ่านการเรียกใช้คลาส .NET ที่ผู้โจมตีกำหนดขึ้นเอง

ความเคลื่อนไหวดังกล่าวเกิดขึ้นในช่วงที่ทั้ง Defused Cyber และ Previdian (ชื่อเดิมคือ KEVIntel) ออกมาเตือนถึงความพยายามโจมตีที่กำลังเกิดขึ้นกับ CVE-2026-8452 โดย Previdian ระบุในโพสต์บน LinkedIn ว่าผู้โจมตีได้ติดตั้ง Web Shell ที่ชื่อว่า x.php และ z.php พร้อมกับรันคำสั่งสำหรับตรวจสอบระบบ เช่น id และ echo

ข้อมูลจากระบบตรวจวัดแสดงให้เห็นว่า ตลอดช่วง 12 วันที่ผ่านมาพบความพยายามโจมตี 36 ครั้งจากที่อยู่ IP ของผู้โจมตีที่แตกต่างกัน 12 ราย โดยมาจากสวิตเซอร์แลนด์ เยอรมนี ฮ่องกง ญี่ปุ่น เนเธอร์แลนด์ รัสเซีย สิงคโปร์ ตุรกี สหรัฐฯ และเวียดนาม

การเพิ่ม CVE-2022-0995, CVE-2015-5287, CVE-2015-3246 และ CVE-2021-23758 ลงในรายการ KEV เกิดขึ้นหลังจาก Cisco Talos เผยแพร่รายงานเกี่ยวกับกลุ่มอาชญากรไซเบอร์จากจีนที่รู้จักกันในชื่อ UAT-10147 ซึ่งกำลังมุ่งเป้าไปที่ Web Server ที่ใช้ Windows และ Linux ทั่วโลก โดยมีเป้าหมายในภาคการศึกษา สื่อ เทคโนโลยี และเกม

ขณะนี้ยังไม่มีข้อมูลสาธารณะที่ระบุว่า CVE-2019-1068 กำลังถูกนำไปใช้โจมตีจริงในรูปแบบใด CISA ขอให้หน่วยงาน Federal Civilian Executive Branch (FCEB) ดำเนินการติดตั้งการแก้ไขสำหรับ CVE-2019-1068 และ CVE-2026-8452 ภายในวันที่ 29 สิงหาคม 2026 และสำหรับช่องโหว่ที่เหลือภายในวันที่ 9 กันยายน 2026

การเพิ่มช่องโหว่เหล่านี้ยังเกิดขึ้นพร้อมกับที่ CISA เผยแพร่ รายงานการทบทวนช่องโหว่ฉบับใหม่ ซึ่งวิเคราะห์ถึงสาเหตุหลักของซอฟต์แวร์ที่ไม่ปลอดภัย รวมถึงแนวทางที่องค์กรสามารถนำไปใช้แก้ไขปัญหาและป้องกันไม่ให้ช่องโหว่ถูกนำไปใช้โจมตี

จากการวิเคราะห์ข้อมูล CVE ในช่วงปี 2024 และ 2025 ของหน่วยงาน พบว่าช่องโหว่ประเภท Injection กลายเป็นประเภทที่พบมากที่สุด โดยมีจำนวน 7,701 รายการในปี 2024 และเพิ่มขึ้นเป็น 21,019 รายการในปี 2025 นอกจากนี้ CISA ยังเน้นย้ำว่า ผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์ที่เป็นที่รู้จักและมีวิธีแก้ไขแล้ว แต่ยังคงปรากฏอยู่ในระบบที่เปิดให้เข้าถึงจากภายนอก และมีการนำปัญญาประดิษฐ์ (AI) มาใช้เพื่อทำให้กระบวนการโจมตีเป็นแบบอัตโนมัติมากขึ้น

ในปีงบประมาณ 2024 และ 2025 ช่องโหว่ด้าน Memory Safety และการตรวจสอบข้อมูลนำเข้าที่ไม่เหมาะสม ปรากฏอยู่ในรายการ KEV ในสัดส่วนที่สูงกว่าที่พบในฐานข้อมูล CVE โดยรวม CISA ระบุ

สำหรับผู้ให้บริการซอฟต์แวร์ ข้อมูลนี้สะท้อนให้เห็นถึงความสำคัญของการแก้ไขปัญหาที่ต้นเหตุ ซึ่งมักนำไปสู่การถูกโจมตีจริงโดยตรง การลดปัญหาที่เป็นต้นเหตุเหล่านี้ตั้งแต่ขั้นตอนการพัฒนาซอฟต์แวร์ จะช่วยให้ผู้ให้บริการสามารถป้องกันช่องโหว่ที่มีแนวโน้มว่าจะถูกผู้โจมตีนำไปใช้ประโยชน์ได้มากขึ้น

ข้อมูลอ้างอิง

Aug 27, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/cisa-adds-six-exploited-flaws-to-kev.html